

COMPUTER REMOTE-MANAGING METHOD

Publication number: JP2002163162

Publication date: 2002-06-07

Inventor: KAWASHITA MAKOTO

Applicant: HORIZON DIGITAL ENTPR INC

Classification:

- **International:** *G06F13/00; H04L12/56; H04L29/14; G06F13/00; H04L12/56; H04L29/14; (IPC1-7): G06F13/00; H04L12/56; H04L29/14*

- **European:**

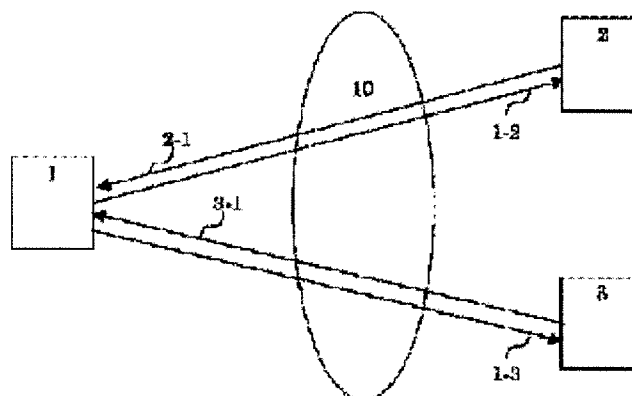
Application number: JP20000357242 20001124

Priority number(s): JP20000357242 20001124

Report a data error here

Abstract of JP2002163162

PROBLEM TO BE SOLVED: To provide a computer remote-managing method having higher security level than a conventional remote-managing method in which a managed computer responds to a demand from a managing computer while standing-by when the managing computer remotely manages the managed computer connected with a communication line such as a computer network, wherein it is unnecessary for the managed computer to open a port number for accepting the demand from the managing computer in the case of remote-monitoring by transmitting information by the managed computer without waiting for the demand from the managing computer and it becomes unnecessary to transmit and receive authenticated information such as a pass-word in the case of remote-operation. **SOLUTION:** In this computer remote-managing method in which the managing computer 1 monitors operation situation of the managed computer 2 by transmitting monitoring information to the managing computer 1 through the communication line 10 by the managed computer 2, the managed computer 2 transmits the monitoring information to the managing computer 1 without accepting a transmission demand from the managing computer 1.



Data supplied from the **esp@cenet** database - Worldwide

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2002-163162
(P2002-163162A)

(43)公開日 平成14年6月7日(2002.6.7)

(51)Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 13/00	3 5 1 3 5 3	G 0 6 F 13/00	3 5 1 N 5 B 0 8 9 3 5 3 B 5 K 0 3 0
H 0 4 L 12/56 29/14	4 0 0	H 0 4 L 12/56 13/00	4 0 0 Z 5 K 0 3 5 3 1 3

審査請求 有 請求項の数 6 O L (全 8 頁)

(21)出願番号 特願2000-357242(P2000-357242)

(22)出願日 平成12年11月24日(2000.11.24)

(71)出願人 500542745
株式会社ホライズン・デジタル・エンタープライズ
東京都渋谷区神山町16番2号
(72)発明者 川下 真
東京都渋谷区道玄坂一丁目12番1号 株式会社ホライズン・デジタル・エンタープライズ内
(74)代理人 100088856
弁理士 石橋 佳之夫

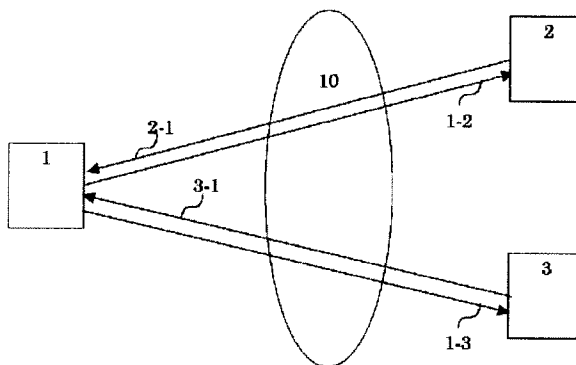
最終頁に続く

(54)【発明の名称】 コンピュータ遠隔管理方法

(57)【要約】

【課題】 管理コンピュータがコンピュータネットワーク等の通信回線に接続された被管理コンピュータを遠隔管理する場合において、被管理コンピュータが待機しながら管理コンピュータからの要求に应答する従来の遠隔管理方法に対して、被管理コンピュータが管理コンピュータからの要求を待つことなく情報を送信するようにしたことにより、遠隔監視の場合において被管理コンピュータは管理コンピュータからの要求を受付けるためのポート番号を開けておく必要がなく、また遠隔操作の場合においてパスワード等の認証情報の送受信が不要となることから、従来の遠隔管理方法に対してセキュリティレベルの高いコンピュータ遠隔管理方法を提供する。

【解決手段】 被管理コンピュータ2が管理コンピュータ1に通信回線10を介して監視情報を送信することで、上記管理コンピュータ1が上記被管理コンピュータ2の稼動状況を監視するコンピュータ遠隔管理方法において、上記管理コンピュータ1から送信要求を受けることなく、上記被管理コンピュータ2が上記管理コンピュータ1に上記監視情報を送信する。



【特許請求の範囲】

【請求項1】 被管理コンピュータが管理コンピュータに通信回線を介して監視情報を送信することで、上記管理コンピュータが上記被管理コンピュータの稼動状況を監視するコンピュータ遠隔管理方法において、
上記管理コンピュータから送信要求を受けることなく、
上記被管理コンピュータが上記管理コンピュータに上記監視情報を送信することを特徴とするコンピュータ遠隔管理方法。

【請求項2】 1つの管理コンピュータが複数の被管理コンピュータを遠隔監視する請求項1記載のコンピュータ遠隔管理方法。

【請求項3】 被管理コンピュータが監視情報を定期的に送信する請求項1または2記載のコンピュータ遠隔管理方法。

【請求項4】 管理コンピュータと被管理コンピュータとの間の通信は暗号化通信とする請求項1、2または3記載のコンピュータ遠隔管理方法。

【請求項5】 監視情報をPOSTメソッドのリクエストとして管理コンピュータに送信する請求項1、2、3または4記載のコンピュータ遠隔管理方法。

【請求項6】 監視情報を受信した管理コンピュータが、指示情報をPOSTメソッドのレスポンスとして被管理コンピュータに送信することで、上記管理コンピュータが上記被管理コンピュータを遠隔操作できるようにした請求項5記載のコンピュータ遠隔管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、管理コンピュータが通信回線を介して被管理コンピュータを遠隔監視、及び遠隔操作するためのコンピュータ遠隔管理方法に関するものである。

【0002】

【従来の技術】近年の通信技術の発達に伴い、コンピュータネットワークをはじめとする各種通信回線に接続するコンピュータ等の情報処理端末の数は増加している。情報処理端末の利用者は、用途や目的に応じて通信先の情報処理端末を選択し、適宜通信プロトコルを使い分けて通信を行う。図8は、コンピュータネットワーク100の利用者が、コンピュータ101を用いてWEBサーバ102、あるいはメールサーバ103に接続している例である。通信101-2、102-1はそれぞれ、プロトコルにHTTP(Hyper Text Transfer Protocol)を用いた通信を示し、通信101-3、103-1はそれぞれ、プロトコルにSMTP(Simple Message Transfer Protocol)、POP3(Post Office Protocol Version 3)を用いた通信を示している。なお、コンピュータ101、102、103がコンピュータネットワーク100と接続す

るための通信回線などについては記載を省略してある(以下、同じ)。

【0003】コンピュータの運用者は、管理対象のコンピュータ(以下、「被管理コンピュータ」という)を正常に稼動させるために、被管理コンピュータの稼動状況を監視しておき、監視結果に応じて適切な対応を採る。また、コンピュータネットワークに接続された複数の被管理コンピュータを運用管理する場合には、コンピュータの運用者は、被管理コンピュータとは別の管理用のコンピュータ(以下、「管理コンピュータ」という)から被管理コンピュータの稼動状況を監視する遠隔監視、あるいは、管理コンピュータから被管理コンピュータを操作する遠隔操作、等の遠隔管理を行うのが一般的である。遠隔監視の方法としては、管理コンピュータから複数の被管理コンピュータに監視情報の送信要求をし、運用者は各被管理コンピュータから受信した監視情報により、各被管理コンピュータの稼動状況等を把握する。監視情報とは、運用者が被管理コンピュータの稼動状況を監視するために必要な情報であり、例えば、被管理コンピュータに予め設定されている「コンピュータの識別名称」や「アドレス情報」等の監視項目からなる管理情報や、監視情報の送信要求を受付けた時点での被管理コンピュータの稼動状況を示す「CPU使用率」や、「プロセス情報」等の監視項目からなる稼動情報、等がある。管理コンピュータが被管理コンピュータに監視情報の送信要求を行い、受け取るための通信プロトコルの例としては、SNMP(Simple Network Management Protocol)がある。図9は、SNMPを利用した通信例を示す図である。ここでは、WEBサーバ102とメールサーバ103の運用者が、コンピュータ104を用いて、WEBサーバ102とメールサーバ103を遠隔監視している例であり、コンピュータ104が管理コンピュータ、WEBサーバ102とメールサーバ103が被管理コンピュータである(SNMPの場合、管理コンピュータはマネージャ、被管理コンピュータはエージェントと呼ばれる)。管理コンピュータ104は、被管理コンピュータ102に対して監視情報の送信要求をする(通信104-2)。監視情報の送信要求を受けた被管理コンピュータ102は、管理コンピュータ104が要求している監視項目をMIB122に基づいて収集し、管理コンピュータ104に送信する(通信102-4)。MIB(Management Information Base)とは、SNMPを利用する場合に、被管理コンピュータが自己の管理情報や稼動情報等を格納しておくデータベースである。通信104-3と103-4は、管理コンピュータ104がSNMPを用いて被管理コンピュータ103を遠隔監視するための通信を示す。また、遠隔操作の方法としては、管理コンピュータから被管理コンピュータに対して指示情報を送信し、指示情報を受信した被管理コ

ンピュータは、指示情報に基づいて動作する。指示情報とは、被管理コンピュータを操作するための情報であり、例えば、「被管理コンピュータに設定されているユーザ情報の変更」あるいは、「被管理コンピュータで動作しているプロセスの終了」等がある。ただし、被管理コンピュータを操作するためには、被管理コンピュータにおける操作のための権限（いわゆるルート権限）が必要であり、遠隔操作の場合、当該権限用のパスワード等の認証情報を指示情報と共に送信することが一般的である。すなわち、被管理コンピュータは、指示情報に基づいて動作する際、いっしょに受信したパスワード等を確認して、当該指示情報の正当性を確認するのである。

【0004】インターネット等の不特定多数の利用者が接続することを前提としたコンピュータネットワークでは、コンピュータネットワークに接続している各コンピュータは、他のコンピュータからの不正アクセスの脅威にさらされる。この不正アクセスを排除するためには、ファイアウォールを設置して接続を制限するのが一般的である。IP (Internet Protocol) を用いた通信の場合、ファイアウォールは、IPパケットを受信すると、IPヘッダに格納されている通信する互いのコンピュータのIPアドレス、あるいはTCPやUDPヘッダに格納されている通信する互いのコンピュータのポート番号を用いて、もしくはIPアドレスとポート番号の組合せ（ソケットという）を用いて接続を制限することが多い。不特定多数の利用者のコンピュータからの接続を前提とするインターネットに接続されたWEBサーバ等のコンピュータの場合は、ファイアウォールは利用者のコンピュータのIPアドレスを予め特定しておくことができないため、ポート番号で接続を制限する、いわゆるポート番号によるフィルタリングを行う。なお、ポート番号には、接続元のポート番号 (Source Port Number) と接続先のポート番号 (Destination port Number) とがあるが、通常ファイアウォールが接続を制限するために用いるポート番号は、接続先のポート番号である。図10を用いてポート番号による接続の制限について説明する。コンピュータ101は、コンピュータネットワーク100を介してWEBサーバ102に接続する。ここで、WEBサーバ102は、ファイアウォール105を介してコンピュータネットワーク100に接続している。ファイアウォール105は、コンピュータネットワーク100からWEBサーバ102へのアクセス要求のIPパケットを受信して接続先のポート番号を確認し、WEBサーバ用のポート番号「80」であれば接続を許可し、それ以外のポート番号であれば接続を拒否するように設定してある（「80」はWell Known Port Numberとして規定されたポート番号）。ここで、コンピュータ101からWEBサーバ102への通信101-2は、接続先のポート番号が「80」

0」を設定したIPパケットであるため、ファイアウォール105は接続を許可し、コンピュータ101は、WEBサーバ102からの応答のIPパケットを受け取ることができる（通信102-1）。

【0005】

【発明が解決しようとする課題】しかしながら、運用者が前述のプロトコルSNMPを用いて管理コンピュータ104からWEBサーバ102を監視する場合、監視情報の送信要求のための通信104-2は、接続先のポート番号がSNMP用の「161」であるため、ファイアウォール105で接続を拒否される（通信105-1は、接続を拒否した旨の通知であり、送信されないこともある）。したがって、運用者はWEBサーバ102の稼動状況を遠隔監視することができない。管理コンピュータ104からWEBサーバ102を遠隔監視するためには、ファイアウォール105に、接続を許可するポート番号として、既に設定されている「80」に加えて「161」を設定する必要がある。

【0006】ただし、ファイアウォールにおいて、接続を許可するポート番号を増やすことは、他のコンピュータからの不正アクセスの機会の増加を招くため、コンピュータセキュリティ上、望ましくない。また、インターネット等のように複数の運用者により管理されているコンピュータネットワークでは、管理コンピュータと被管理コンピュータの通信経路上のすべてのファイアウォールにおいて、ポート番号「161」が接続可能に設定されていることは期待できず、被管理コンピュータの数が増加すれば、遠隔監視を行うことは困難あるいは不可能となる。一方、遠隔操作の場合、指示情報と共にいわゆるルート権限用のパスワード等の認証情報も送信する必要があることから、第三者による盗聴の危険性があり、ひいては被管理コンピュータへの不正アクセスを誘発してしまい、セキュリティ上好ましくない。

【0007】本発明は以上のような従来技術の問題点を解消するためになされたもので、管理コンピュータがコンピュータネットワーク等の通信回線に接続された被管理コンピュータを遠隔管理する場合において、被管理コンピュータが待機しながら管理コンピュータからの要求に応答する従来の遠隔管理方法に対して、被管理コンピュータが管理コンピュータからの要求を待つことなく情報を送信するようにしたことにより、遠隔監視の場合において被管理コンピュータは管理コンピュータからの要求を受け付けるためのポート番号を開けておく必要がなく、また遠隔操作の場合においてパスワード等の認証情報の送受信が不要となることから、従来の遠隔管理方法に対してセキュリティレベルの高いコンピュータ遠隔管理方法を提供することを目的とする。

【0008】

【課題を解決するための手段】請求項1記載の発明は、被管理コンピュータが管理コンピュータに通信回線を介

して監視情報を送信することで、上記管理コンピュータが上記被管理コンピュータの稼動状況を監視するコンピュータ遠隔管理方法において、上記管理コンピュータから送信要求を受けることなく、上記被管理コンピュータが上記管理コンピュータに上記監視情報を送信することを特徴とする。

【0009】請求項2記載の発明は、請求項1記載の発明において、1つの管理コンピュータが複数の被管理コンピュータを遠隔監視することを特徴とする。

【0010】請求項3記載の発明は、請求項1または2記載の発明において、被管理コンピュータが監視情報を定期的に送信することを特徴とする。

【0011】請求項4記載の発明は、請求項1、2または3記載の発明において、管理コンピュータと被管理コンピュータとの間の通信は暗号化通信とすることを特徴とする。

【0012】請求項5記載の発明は、請求項1、2、3または4記載の発明において、監視情報をPOSTメソッドのリクエストとして管理コンピュータに送信することを特徴とする。

【0013】請求項6記載の発明は、請求項5記載の発明において、監視情報を受信した管理コンピュータが、指示情報をPOSTメソッドのレスポンスとして被管理コンピュータに送信することで、上記管理コンピュータが上記被管理コンピュータを遠隔操作できるようにしたことを特徴とする。

【0014】

【発明の実施の形態】以下、図面を参照しながら本発明にかかるコンピュータ遠隔管理方法の実施の形態について説明する。図1は、本発明にかかるコンピュータ遠隔管理方法の実施の形態を示したブロック図である。符号1は管理コンピュータを示し、符号2、3は被管理コンピュータを示す。また、符号10は通信回線を示し、管理コンピュータ1と被管理コンピュータ2、3とは、それぞれ通信回線10を介して通信する。通信回線10には、インターネットやLAN(Local Area Network)等のコンピュータネットワークや、電話回線、衛星通信回線等がある。被管理コンピュータ2、3は、それぞれHTTPのPOSTメッセージのリクエストを送信でき、またPOSTメッセージのレスポンスを受信できるものであり、一方管理コンピュータ1は、POSTメッセージのリクエストを受信して、POSTメッセージのレスポンスを送信できるものである。管理コンピュータ1や被管理コンピュータ2、3の例としては、LinuxやWindows等が動作するパソコンや、UNIX(登録商標)マシン、あるいは、携帯電話やPDA等の携帯情報処理端末等がある。ただし、管理コンピュータ1や被管理コンピュータ2、3の動作する機器としてはこれらに限定されるものではなく、先の条件に該当するものであればよい。なお、図1は

つの管理コンピュータ1が2つの被管理コンピュータ2、3を遠隔管理する例を示しているが、1つの管理コンピュータにより遠隔管理される被管理コンピュータの数はこれに限定されるものではなく、用途や目的等に応じて適宜1以上の被管理コンピュータを選定できる。

【0015】図2は図1の実施の形態における通信の順序を時系列で示した図であり、図の上方から下方に向かう順に通信が行われることを示している。図2を用いて、図示しない被管理コンピュータ2、3の運用者が、管理コンピュータ1を用いて被管理コンピュータ2の稼動状況を遠隔監視する方法について説明する。まず、被管理コンピュータ2が監視情報をHTTPのPOSTメソッドのリクエストとして管理コンピュータ1に送信する(通信2-1)。ここで監視情報とは、運用者が被管理コンピュータ2の稼動状況を遠隔監視するために必要な情報であり、管理情報と稼動情報とからなる。管理情報とは、運用者が被管理コンピュータ2に予め設定している情報であり、例えば「コンピュータの識別名称」や「アドレス情報」等の監視項目からなる。また、稼動情報とは、被管理コンピュータ2の稼動状況を示す情報であり、例えば「CPU使用率」や「プロセス情報」等の監視項目からなる。図3、4は、それぞれ管理情報と稼動情報の監視項目の例である。なお、監視項目はこれらに限定されるものではなく、運用者が適宜決定する。また監視項目は、遠隔監視をはじめた後においても、運用者が適宜変更できる。

【0016】被管理コンピュータ2から監視情報を受信した管理コンピュータ1は、図示しないコンピュータプログラムを用いて、当該監視情報を処理する。処理の内容は、受信した監視情報の各監視項目について、予め設定してある各監視項目のしきい値との比較、あるいは、受信した監視情報を図示しない管理コンピュータ1内部の情報記憶装置に格納する等があり、運用者が適宜決めておく。

【0017】監視情報を処理した管理コンピュータ1は、結果情報をPOSTメソッドのレスポンスとして被管理コンピュータ2に送信する(通信1-2)。結果情報とは、管理コンピュータ1が監視情報を処理した結果を被管理コンピュータ2に通知するためのものである。結果情報を受信した被管理コンピュータ2は、先に送信(通信2-1)した監視情報を管理コンピュータ1が処理できたか否かの確認等ができる。以上説明したように、本発明にかかるコンピュータ遠隔管理方法においては、被管理コンピュータは管理コンピュータからの要求を受付けるためのポートを開けておく必要がなく、セキュリティレベルの向上を図ることができる。また、管理コンピュータ1と被管理コンピュータ2との間の通信2-1、1-2は、コンピュータネットワークでの利用度が極めて高く、そのためファイアウォールで接続を制限されることがないHTTP(その中のPOSTメソッド)

ド)を用いているため、管理コンピュータ1と被管理コンピュータ2との通信経路上にファイアウォールが設置されていたとしても、管理コンピュータ1が被管理コンピュータ2を遠隔監視する上で支障はない。管理コンピュータ1が被管理コンピュータ3を遠隔監視する場合も、通信3-1-、1-3により同様に行える。なお、管理コンピュータ1と被管理コンピュータ2、3との間で送受信される監視情報、結果情報のフォーマット等については、予め決めておく。

【0018】図1の実施の形態において、被管理コンピュータ2あるいは3が監視情報を管理コンピュータ1に送信するタイミングを、例えば「5分間隔」、「毎週月曜日の朝7時」等、定期的としてもよいし、監視項目がしきい値を超えた場合、例えば「ディスク使用率が75%に達した時」等、不定期としてもよい。定期的とすると、監視情報の送信間隔を短くすることで、管理コンピュータ1は、被管理コンピュータ2、3の稼動状況を常に監視することができる。一方不定期とすると、必要となときに監視情報を送信する等、管理コンピュータ1と被管理コンピュータ2、3の双方に処理負担が少なくなり、また、通信回線10の通信トラフィックを抑えることもできる。運用者は、監視情報の送信のタイミングを定期的、不定期、あるいは両者を組み合わせる等、遠隔監視の目的等に応じて決める。

【0019】また図1の実施の形態において、管理コンピュータ1と被管理コンピュータ2、3との間の通信は、SSL(Secure Socket Layer)等を用いた暗号化通信としてもよい。暗号化通信とすることで、第三者による管理コンピュータ1と被管理コンピュータ2、3との間の通信が盗聴されるのを排除できるため、通信の安全性を高めることができる。なお、管理コンピュータ1と被管理コンピュータ2、3との間の通信にHTTPを用いる場合、HTTPとSSLとの親和性が高いことから、SSLの実装は容易となる。

【0020】さらに図1の実施の形態において、被管理コンピュータ2と被管理コンピュータ3が管理コンピュータ1に送信する監視情報の監視項目は、一致してもよいし、一致していなくてもよく、運用者が遠隔監視の目的等に応じて適宜決める。

【0021】図1の実施の形態によれば、被管理コンピュータ2が管理コンピュータ1に通信回線を介して監視情報を送信することで、上記管理コンピュータ1が上記被管理コンピュータ2の稼動状況を監視するコンピュータ遠隔管理方法において、上記管理コンピュータ1から送信要求を受けることなく、上記被管理コンピュータ2が上記管理コンピュータ1に上記監視情報を送信することで、被管理コンピュータ2は管理コンピュータ1からの要求を受付けるためのポート番号を開けておく必要がなく、セキュリティレベルの向上を図ることができる。

また、被管理コンピュータ2は、管理コンピュータ1とは無関係に管理コンピュータ1に監視情報を送信できるので、送信するタイミングを定期的とすると、運用者は、被管理コンピュータ2の稼動状況の時間的変化を容易に把握でき、遠隔監視の効果を高めることができる。

【0022】また、監視情報をPOSTメソッドのリクエストとして管理コンピュータ1に送信することで、管理コンピュータ1と被管理コンピュータ2との通信経路上にファイアウォールが設置されていた場合でも、接続を制限されることなく遠隔監視が実現でき、遠隔監視とファイアウォールの並行運用が可能となる。

【0023】次に、本発明にかかるコンピュータ遠隔管理方法の別の実施の形態について説明する。図1の実施の形態は、管理コンピュータが被管理コンピュータから監視情報を受信するものであったが、本実施の形態は、管理コンピュータが被管理コンピュータから監視情報を受信するのに加えて、さらに被管理コンピュータを遠隔操作するものである。図5は、本実施の形態における管理コンピュータ1と被管理コンピュータ4との通信の順序を時系列で示した図である。なお、管理コンピュータ1と被管理コンピュータ4とが通信回線を介して互いに通信できるのは、図1の実施の形態と同様である。被管理コンピュータ4が管理コンピュータ1に監視情報を送信する「通信4-1」は、図1の実施の形態の「通信2-1」と同様である。図1の実施の形態との違いは、監視情報を受信(通信4-1)した管理コンピュータ1は、当該監視情報を処理した後に、結果情報を送信せずに指示情報を被管理コンピュータ4に送信(通信1-4-1)する。指示情報とは、管理コンピュータ1が被管理コンピュータ4を遠隔操作するための情報であり、例えば特定の監視項目に関する情報の送信の指示、あるいは、先に送信した監視情報の再送信、等がある。指示情報を受信した被管理コンピュータ4は、当該指示情報が、先の通信4-1のレスポンスとして送信されていることを確認して、指示情報の内容に基づいて動作する。ここでは、監視情報を管理コンピュータ1に送信する例を示している(通信4-1-1)。監視情報を受信した管理コンピュータ1は、さらに別の指示情報を送信してもよいし、結果情報を送信してもよい。図5は、2度の指示情報を送信(通信1-4-1、1-4-2)した後に、結果情報を送信(通信1-4)しているが、指示情報の送信回数は、これに限定されるものではない。なお、通信1-4で送信する結果情報は、図1の実施の形態における「通信1-2」で送信する結果情報と同様のものである。

【0024】図6は、本実施の形態における管理コンピュータ1と被管理コンピュータ4との別の通信の順序を時系列で示した図である。図5の通信との違いは、監視情報を受信(通信4-1-1)した管理コンピュータ1は、結果情報を送信せずに被管理コンピュータ4に指示

情報付き結果情報を送信（通信 1-4-0）する点である。指示情報付き結果情報とは、図 5 の通信における指示情報を含んだ結果情報であり、指示情報付き結果情報を受信した被管理コンピュータ 4 は、管理コンピュータ 1 が監視情報を処理した結果を判断すると共に、指示情報に基づいて動作する。ただし、指示情報付き結果情報に基づいた動作には、監視情報を管理コンピュータ 1 に送信することは含まない。指示情報の内容としては、例えば被管理コンピュータ 4 のシステム再起動、被管理コンピュータ 4 の特定プロセスの終了、あるいは、被管理コンピュータ 4 のハードディスク内部のデータの外部記憶装置への退避、等がある。なお図 6 では、1 度の指示情報を送信（通信 1-4-1）した後に指示情報付き結果情報を送信（通信 1-4-0）しているが、指示情報の送信をすることなく、監視情報を受信（通信 4-1）した後に、指示情報付き結果情報を送信することもできる。

【0025】図 7 は、本実施の形態における管理コンピュータ 1 と被管理コンピュータ 4 とのさらに別の通信の順序を時系列で示した図である。図 5 の通信との違いは、被管理コンピュータ 4 が、監視情報ではなく、指示待ち情報を先ず管理コンピュータ 1 に送信（通信 4-0）する点である。指示待ち情報とは、被管理コンピュータ 4 が管理コンピュータ 1 に対して指示情報の送信を依頼するための情報である。指示待ち情報を受信した管理コンピュータ 1 は、指示情報を被管理コンピュータ 4 に送信（通信 1-4-1）する。指示情報を受信した被管理コンピュータ 4 は、図 6 の通信の場合と同様に指示情報に基づいて動作する。ここで、指示待ち情報を受信した管理コンピュータ 1 は、指示情報を送信する代わりに、図 6 の指示情報付き結果情報を送信することもできる。また、遠隔操作の必要がない場合には、単に結果情報を送信することもできる。なお、本実施の形態における指示情報、指示情報付き結果情報、および指示待ち情報のフォーマット等については、予め決めておく。

【0026】以上説明した実施の形態によると、監視情報を受信した管理コンピュータ 1 が、指示情報を POST メソッドのレスポンスとして被管理コンピュータ 4 に送信することで、上記管理コンピュータ 1 が上記被管理コンピュータ 4 を遠隔操作できるようにしたため、管理コンピュータ 1 と被管理コンピュータ 4 との間で遠隔操作のためのパスワード等の送受信が不要となり、セキュリティレベルの向上を図ることができる。

【0027】

【発明の効果】請求項 1 記載の発明によれば、被管理コンピュータが管理コンピュータに通信回線を介して監視情報を送信することで、上記管理コンピュータが上記被管理コンピュータの稼動状況を監視するコンピュータ遠隔管理方法において、上記管理コンピュータから送信要求を受けることなく、上記被管理コンピュータが上記管

理コンピュータに上記監視情報を送信することで、被管理コンピュータは管理コンピュータからの要求を受付けるためのポート番号を開けておく必要がなく、セキュリティレベルの向上を図ることができる。また、被管理コンピュータは、管理コンピュータとは無関係に管理コンピュータに監視情報を送信できるので、運用者は、被管理コンピュータの稼動状況の時間的な変化を容易に把握でき、遠隔監視の効果を高めることができる。

【0028】請求項 5 記載の発明によれば、請求項 1、2、3 または 4 記載の発明において、監視情報を POST メソッドのリクエストとして管理コンピュータに送信することで、管理コンピュータと被管理コンピュータとの通信経路上にファイアウォールが設置されていた場合でも、接続を制限されることなく遠隔監視が実現でき、遠隔監視とファイアウォールの並行運用が可能となる。

【0029】請求項 6 記載の発明によれば、請求項 5 記載の発明において、監視情報を受信した管理コンピュータが、指示情報を POST メソッドのレスポンスとして被管理コンピュータに送信することで、上記管理コンピュータが上記被管理コンピュータを遠隔操作できるようにしたため、管理コンピュータと被管理コンピュータとの間で遠隔操作のためのパスワード等の送受信が不要となり、セキュリティレベルの向上を図ることができる。

【図面の簡単な説明】

【図 1】本発明にかかるコンピュータ遠隔管理方法の実施の形態を示すブロック図である。

【図 2】図 1 の実施の形態における通信の順序を時系列で示したフローチャート図である。

【図 3】図 1 の実施の形態における管理情報の監視項目の例である。

【図 4】図 1 の実施の形態における稼動情報の監視項目の例である。

【図 5】本発明にかかるコンピュータ遠隔管理方法の別の実施の形態における通信の順序を時系列で示したフローチャート図である。

【図 6】本発明にかかるコンピュータ遠隔管理方法の別の実施の形態における別の通信の順序を時系列で示したフローチャート図である。

【図 7】本発明にかかるコンピュータ遠隔管理方法の別の実施の形態におけるさらに別の通信の順序を時系列で示したフローチャート図である。

【図 8】従来のコンピュータ遠隔管理方法を説明するためのブロック図である。

【図 9】従来のコンピュータ遠隔管理方法の例について示すブロック図である。

【図 10】従来のコンピュータ遠隔管理方法の例について示すブロック図である。

【符号の説明】

1 管理コンピュータ
2 3 4 被管理コンピュータ

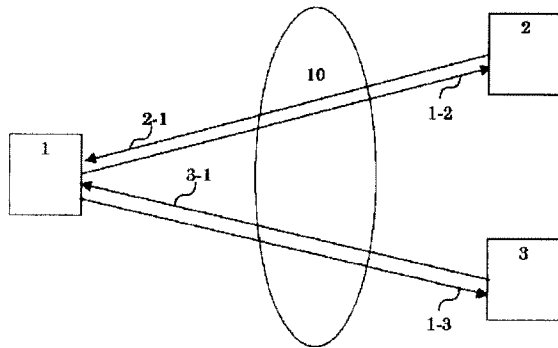
11

12

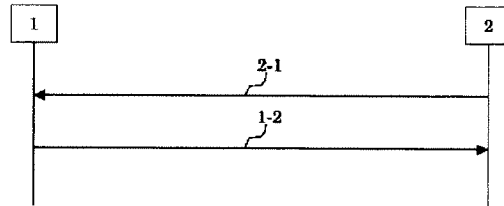
10

通信回線

【図1】



【図2】



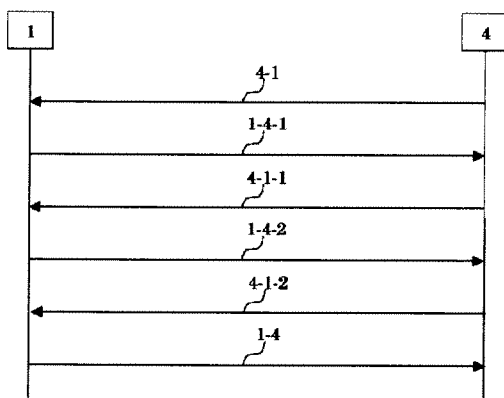
【図4】

【図3】

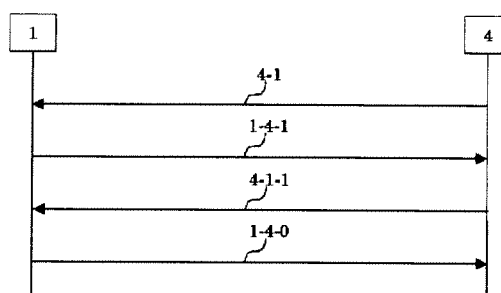
インベントリ管理	識別名 ホスト名 ドメイン名 コメント IPアドレス MACアドレス 稼働時間 接続ユーザー情報 CPU情報 HDD情報 NIC情報 カーネルバージョン情報 ディストリビューション情報 rpm情報
障害報告管理	障害報告の管理
ログ管理	LCBログ管理機能
ジョブ管理	LC設定配信 rpm配信 配信予約 配信履歴 電源管理
レポートイング	レポート発行機能
ヘルプデスク	高機能な障害報告管理

ステータス監視	システム負荷 CPU使用率 HDD Read HDD Write NIC In NIC Out 物理メモリ使用量 仮想メモリ使用量
リソース監視	HDD 使用量 物理メモリ使用量 仮想メモリ使用量 CPU使用量
プロセス監視	プロセス情報 プロセス監視 未知のプロセスの監視
セキュリティ監視	ポート情報 ログ監視 ログイン監視
サービス監視	Ping Socket Ping Trace Route
障害報告一覧	監視項目に対する注意・警告一覧
ハードウェア監視	CPUの温度監視 筐体内部の温度監視 ファンの回転数監視 HDD障害監視
Oracle監視	DBの状態監視

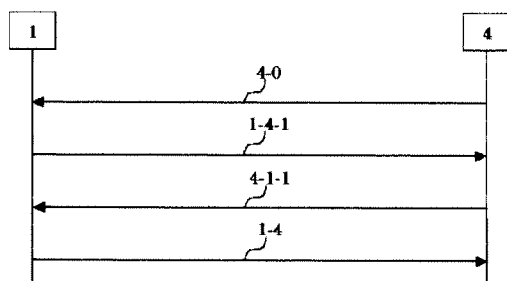
【図5】



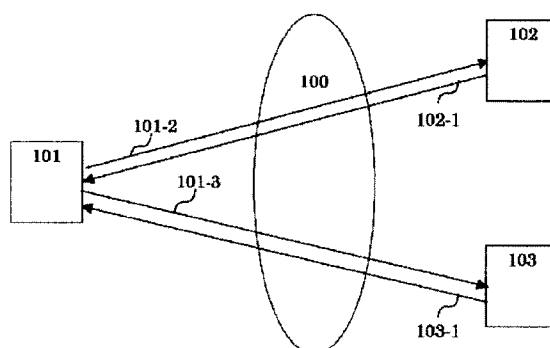
【図6】



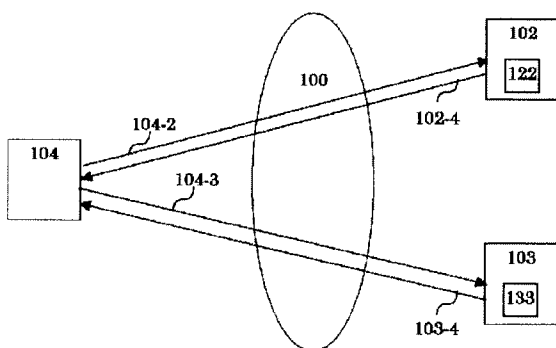
【図7】



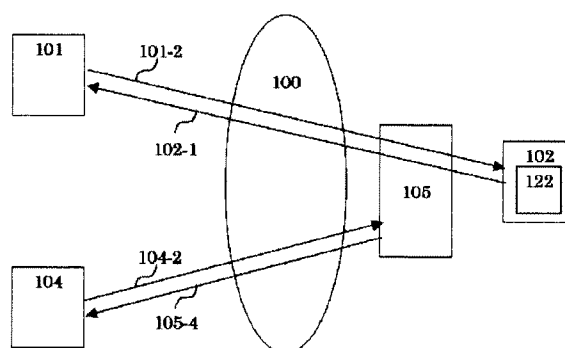
【図8】



【図9】



【図10】



フロントページの続き

F ターム(参考) 5B089 GA11 GA21 GB02 HB06 JA35
 JB16 KA13 KC30 KH30
 5K030 GA04 GA08 GA16 HA11 HB06
 HC01 HD03 LE07 MA06 MC09
 5K035 AA02 AA04 AA07 BB02 CC01
 CC03 CC10 DD01 FF01 MM03
 MM07